

ABSTRACT OF THE DISCLOSURE

[67] A ticket-based secure time protocol is used to provide client devices, or users, with secure time signals. In a preferred embodiment, the secure time signals are provided by a secure time server so that multiple clients can be time-synchronized. Ticket-based authentication uses digital certificates and public key cryptography, such as Elliptic Curve Cryptography (ECC) to reduce key administration overhead and decryption processing. Standard authentication architectures and approaches, such as Kerberos, can be used for some aspects of the invention. A preferred embodiment uses Request and Reply messages that provide added security and functionality, such as authentication, sequence-checking and verification of target destination.